1. (Four time Amended) A method for protecting software from unauthorised use, comprising the steps of:

determining if identity means/information, is existing in a processing [device] apparatus ;

using a favourable result of said determination as a pre-condition for said processing [device] apparatus providing user access to said software desired to be protected ;

wherein said identity means/information being used by a control means of said processing [device for] apparatus in enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity means/information being specific to said rightful user(s) .

3. (Third time Amended) A method for protecting software from unauthorised use , as claimed in claim 12, wherein said software desired to be protected being first software used on said processing [device] apparatus for determining third information related to hardware and/or software of said processing [device] apparatus ;

wherein further comprising second software for, when being executed, authenticating the computer on which said second software runs as being said processing [device] apparatus, basing on at least a part of said third information;

and access to third software will be provided if said authentication result is favourable .

6. (Second time Amended) A method for protecting software from unauthorised use , as claimed in claim 5, wherein said processing [device] apparatus having an encrypted identity of its rightful user ; and if one of said protected programs stored in said [computer] processing apparatus has a valid user identity which being not consistent with the decryption result of said encrypted identity of said processing [device] apparatus, use of said protected programs will not be permitted and will be permitted if otherwise .

7. (Four time Amended) Protection software for use on a processing [device] apparatus, to protect software publicly distributed [by a system] against unauthorised use ;

said protection software comprising :

identity software used on said processing [device] apparatus in enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

authorising software effectively under the control of said rightful user(s) [the user thereof] for, when executed, providing user access to said software desired to be protected ;

wherein said identity software and said authorising software are contained in said protection software in such a manner that said authorising software is prevented from being copied therefrom individually; and

wherein the improvement resides in said protection [depends] basing on no hardware and/or software specific to said rightful user(s) other than said identity software and said identity software being specific to said rightful user(s) .

10. (Four time Amended) Authorising program/means used in a processing [device] apparatus, to protect other software against unauthorised use ;

said authorising program/means being for providing access to said software desired to be protected ;

wherein information specific to rightful user(s) of said software desired to be protected, exists in said authorising program/means and being accessible to the user thereof ;

said information being capable of being used, but not in a form [to be] as for being so used , by said processing [device] apparatus in enabling operation(s) for which said rightful user(s) has to be responsible .

12. (Third time Amended) A method for protecting software from unauthorised use , comprising the steps of :

obtaining a first information from a user of a processing [device] apparatus having an identity software/means ;

using said first information received being correct as a pre-condition for said processing [device] apparatus providing user access to said software desired to be protected;

wherein said identity software/means being for providing a second information specific to rightful user(s) of said software desired to be protected, if said correct first information is being obtained from a user thereof ;

and said second information being used by said processing [device] apparatus in enabling operation(s) for which said rightful user(s) has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed.

14. (Third time Amended) A method for protecting software from unauthorised use , comprising the steps of :

authenticating identity information/means associated with a control means of a processing [device] apparatus;

using a favourable result of said authentication as a pre-condition for said [control means] processing apparatus providing user access to said software desired to be protected ;

wherein said identity information/means being used by said control means [for] in enabling operation(s) for which rightful user(s) of said software desired to be protected has to be responsible ;

wherein access to said software desired to be protected is being provided without causing a said operation being performed and said identity information/means being specific to said rightful user(s) .

16. (Four time Amended) A method for protecting software [distributed by a system] from unauthorised use , comprising the steps of :

a) creating first software with [said] confidential information of a rightful [user(s)] user of said software desired to be protected therein ;

b) running said first software on a processing [device] apparatus ;

c) obtaining by said first software running on said processing [device] apparatus, first information from the user thereof ;

d) determining by said first software, from said processing [device] apparatus second information related to the hardware or/and software thereof for future reference in step [f)] e) below, in response to said first information obtained being consistent with said confidential information therein ;

e) thereafter, authenticating by second software, the processing [device] apparatus onwhich said second software is being used, basing on at least a part of said second information ;

f) using, by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on the processing [device] apparatus onwhich said second software is being used ;

wherein said confidential information [is] being necessary for enabling electronic transaction(s) for which said rightful [user(s)] user has to be responsible ; and said steps c) to f) is being performed without causing a said transaction take place .

18. (Second time Amended) A method for protecting software from unauthorised use, comprising the steps of :

a) [transferring from a software distribution system,] supplying said software desired to be protected to a processing apparatus [device] ;

b) [transferring from said software distribution system, first and] supplying first software and second software which being specific to a user, to said processing [device] apparatus ;

c) establishing a communication between said first software running on said processing [device] apparatus, and [a control means of] a remote electronic transaction system ;

d) verifying said user having a valid account, by [said control means of] said remote electronic transaction system to said first software ;

e) using by said first software, a favourable result of said verification as a pre-condition for determining from said processing [device] apparatus information related to the hardware or/and software thereof, for future reference in step f) below ;

wherein a cost is being charged from said user [by said software distribution system,] for the first time said steps a) to e) being carried out ; thereafter

f) authenticating by said second software, the processing [device] apparatus onwhich said second software is being used, say, second processing [device] apparatus, basing on at least a part of said information related to said hardware or/and software ;

g) using by said second software, a favourable result of said authentication as a pre-condition for permitting use of said software desired to be protected on said second processing [device] apparatus, with no charge ;

if the result of said authentication is not favourable, repeat at least said steps c) to [g)] e) with said second processing [device] apparatus, without re-charging from said user said cost .

19. (Second time Amended) A method for protecting software from unauthorised use, as claimed by claim 18, wherein no charge by said software distribution system for repeating at least said steps c) to [g]] e) .

20. (Third time Amended) A method for protecting software [distributed by a system] from unauthorised use, comprising the steps of :

a) creating [by said system,] first software ;

wherein "the presence of identity information/means which being specific to a rightful user of said software desired to be protected and being used [for] in enabling operation(s) for which said rightful user has to be responsible, in a processing [device] apparatus" is being used in the creation of said first software as a pre-condition for said first software to perform step c) below ;

b) [transferring from said system,] running said first software [to] on said processing [device] apparatus ;

c) determining by said first software running on said processing [device] apparatus meeting said precondition, first information related to the hardware or/and software of said processing [device] apparatus, for future reference in step e) below ;

d) thereafter, determining by second software, from the processing [device] apparatus onwhich said second software is being used, second information related to the hardware or/and software thereof;

e) determining by said second software, if said second information is consistent with said first information ;

f) using by said second software, a favourable result of said determination of consistence as a pre-condition for permitting use of said software desired to be protected on the processing [device] apparatus onwhich said second software is being used ;

repeat at least said [steps] step c) with the processing apparatus on which said second software is being used [to f)] if said result of said determination of consistence is not favourable, without causing **any** operation(s) for which said rightful user has to be responsible, being performed ;

wherein said first and second software being specific to said rightful user.